SAML Artifact Profile
as an Adopted Scheme
for eAuthentication

11/3/2003
Draft Version 0.0.1

Document History

Status	Release	Date	Comment	Audience
Pilot	0.0.1	11/3/03	Initial draft of the document, adapted from proposed SAML artifact architecture document proven in the interoperability lab.	Limited

Editors

Chris Louden

Dave Silver

Table Of Contents

SAML ARTIFACT PROFILE ..... **I**

AS AN ADOPTED SCHEME ..... **I**

FOR EAUTHENTICATION ..... **I**

DOCUMENT HISTORY ..... **II**

EDITORS ..... **II**

TABLE OF CONTENTS ..... **III**

1 INTRODUCTION **1**

1.1 TERMS 2

2 ARCHITECTURE DESCRIPTION **3**

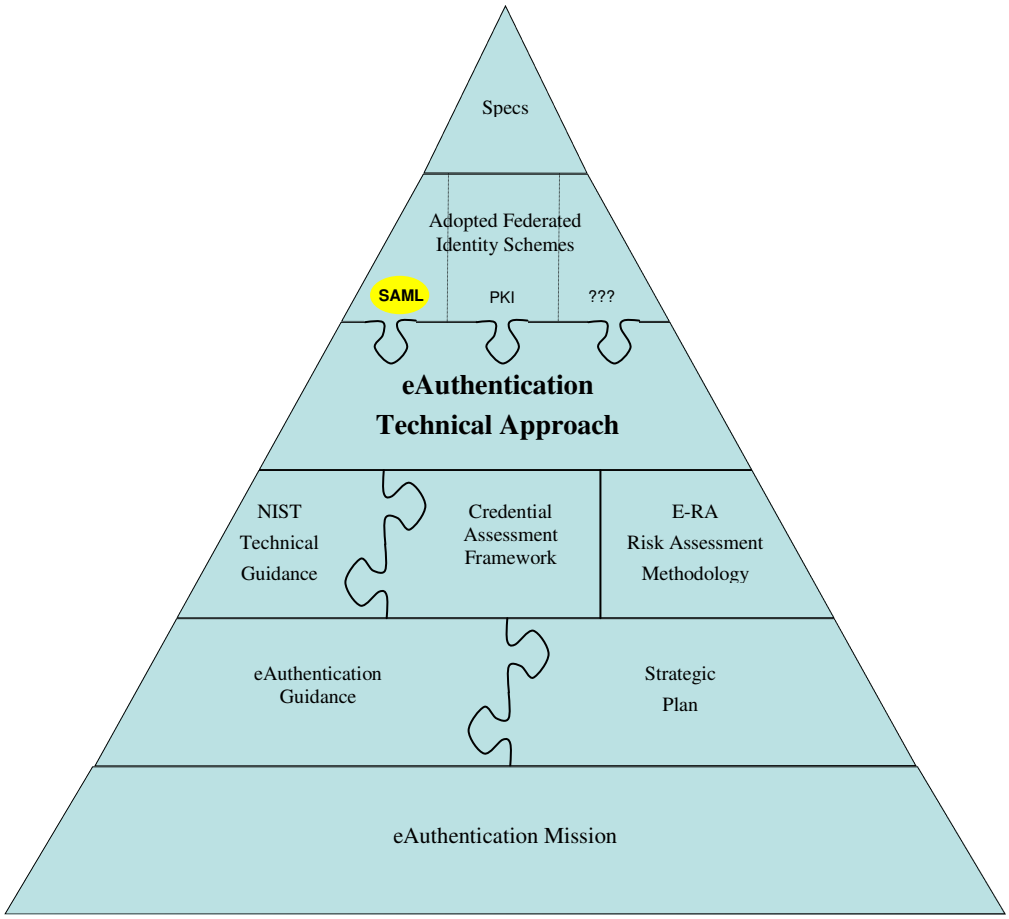
3 SINGLE SIGN-ON **4**

4 GOVERNANCE **5**

1 INTRODUCTION

This paper provides an overview of the use of the SAML Artifact Profile in the eAuthentication Initiative. The SAML Artifact Profile is one of the adopted schemes within the eAuthentication architectural framework.

This document is part of a suite of documents for the eAuthentication initiative. The figure below shows where this document fits into the overall documentation suite. For more information please refer to the eAuthentication Technical Approach. Current versions of these documents are available on the eAuthentication website at http://www.cio.gov/eAuthentication/.



1.1 Terms

This document relies on terminology defined in the NIST E-Authentication Technical Guidance and the OMB Guidance for E-Authentication. The following terms have special meaning in this context:

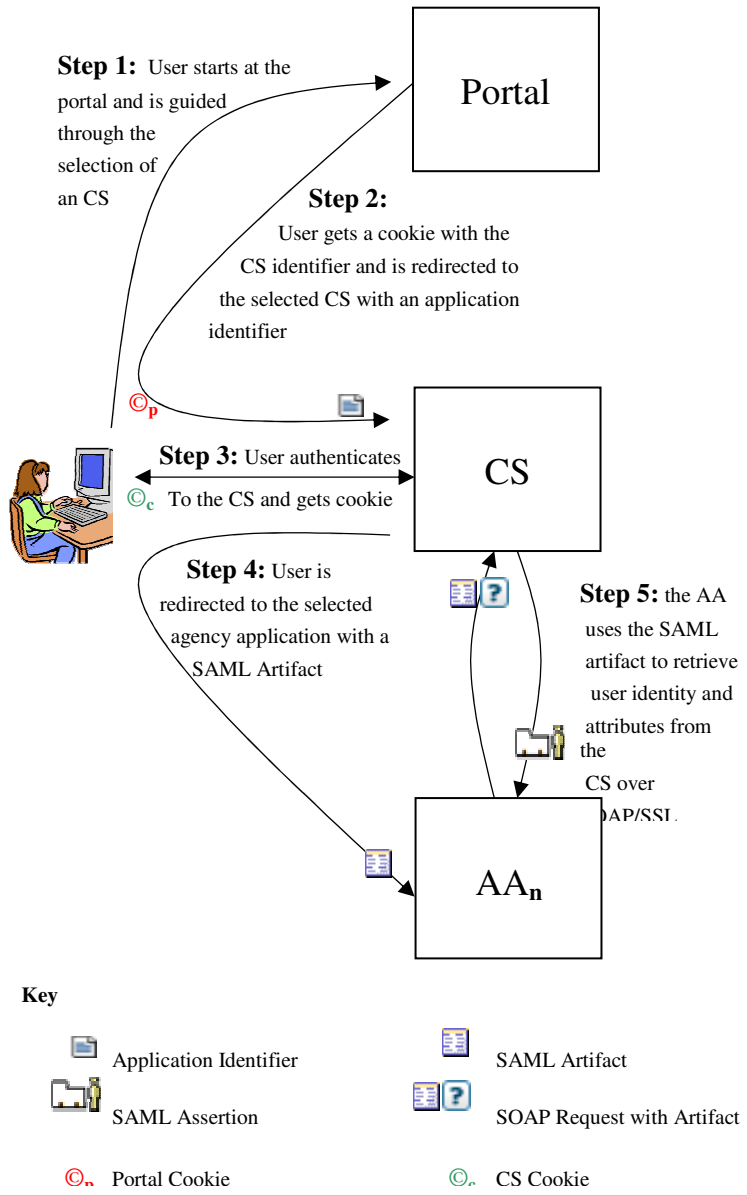
Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires a user to be authenticated.
Credential Service (CS)	A service of an Credential Service Provider (CSP) that provides credentials to subscribers for use in electronic transactions. If a CS offers more than one type of credential then each one is considered a separate CS.
Credential Service Provider (CSP	An organization that offers one or more Credential Services (CSs).

2 ARCHITECTURE DESCRIPTION

Figure 1 illustrates the initial process of authentication using this architecture. The unauthenticated user begins at the portal. The role of the portal in this architecture is consistent with typical portal functions; it helps the end user find the resources they are interested in. While interacting with the portal the user makes two decisions, which Agency Application (AA) they would like to use and which Credential Service Provider (CS) they would like to use. The portal has access to the list of AAs and the authentication level required by each, as well as the list of CSs and the authentication level of their credentials.

Once users make their selections at the portal they are redirected to the selected credential provider with an Application Identifier. The Application Identifier is simply a pointer or identifier to a particular AA, it is not sensitive and does not contain personal information. The Application Identifier is included in the query string of the redirect, making it available to the CS. The redirect also assigns a session cookie to the user indicating which CS they have selected for the required authentication level. The cookie is not sensitive and does not contain any personal information; it is used to facilitate single sign-on in later transactions.

Figure 1: First Transaction



The CS then authenticates the user and assigns a session cookie to the user, which is also used to facilitate single sign-on. The contents and sensitivity of the CS cookie would vary among CSs. Once the authentication is complete the user is redirected to the AA indicated by the application identifier passed from the portal.

The redirection to the AA includes a SAML artifact, which is used by the AA to retrieve SAML assertions containing the identity and attributes of the user. Once the assertions are retrieved the user is authenticated and can begin interacting with application.

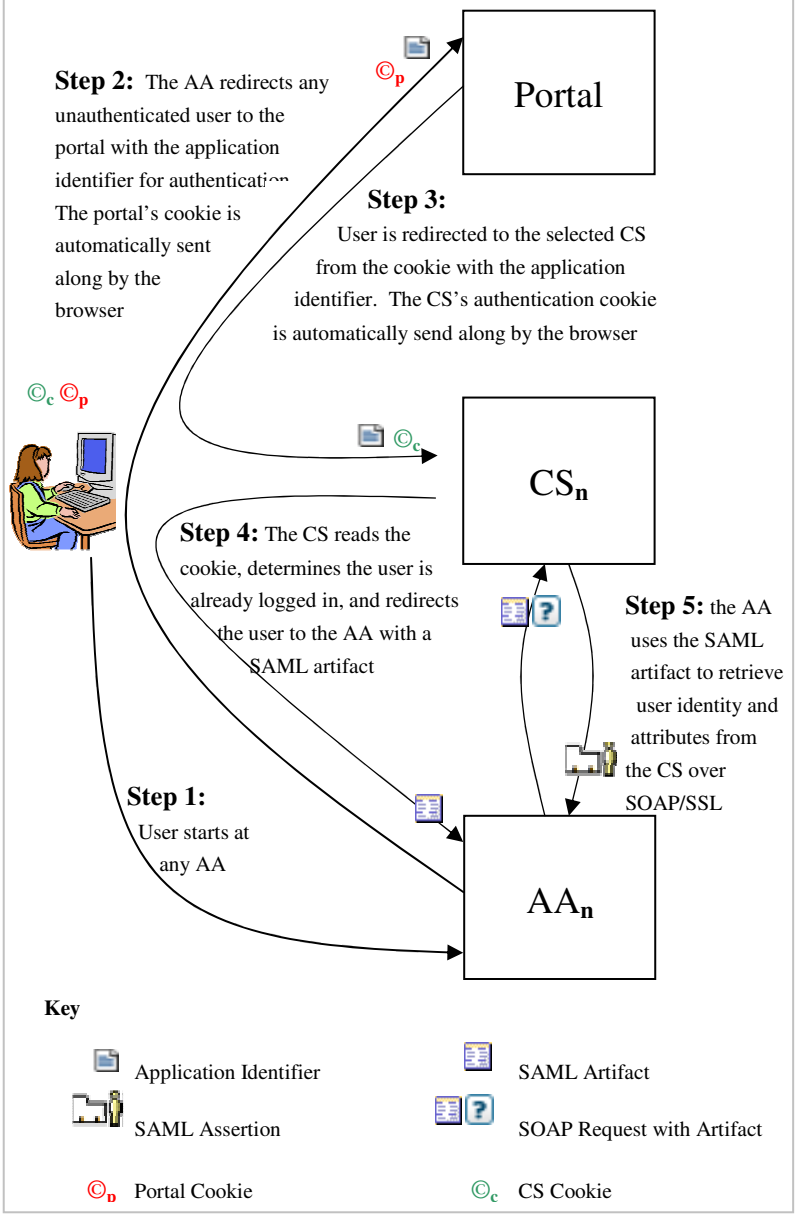
The last two steps of the process are specified by the SAML Artifact Profile.

3 SINGLE SIGN-ON

Figure 2 illustrates how single sign-on works in this architecture. After initial authentication with the CS the user is seamlessly logged into any other AAs of equal or lower authentication levels as needed.

The diagram begins with the user accessing an AA directly. The AA redirects any unauthenticated user to the Portal with its own application identifier in the query string. Since the user has already authenticated they possess a portal cookie that indicates which CS they selected in their last session. The principle function of the portal interface is to help the user select the AA and CS they are want to use, which is not necessary in this case. Since the AA provided the application identifier and the cookie provides the CS selection the portal can immediately redirect the user to the CS as described in the previous section without requesting any further information from the user.

Figure 2: Subsequent Transactions



When the user arrives at the CS they will present the cookie assigned in the previous authentication. The CS reads the cookie to determine the user's identity without requesting another authentication. Once the cookie is deciphered the user is redirected with the SAML artifact as described in the previous section. Once again there is no need to request any further information from the user. Optionally, the CS could notify the user they are about to be logged into the AA and provide an opportunity to decline.

Finally the user ends up back at the AA where they started, but this time they have the SAML Artifact included in the query string. The AA can then use the artifact to retrieve the SAML assertions from the CS, authenticating the user.

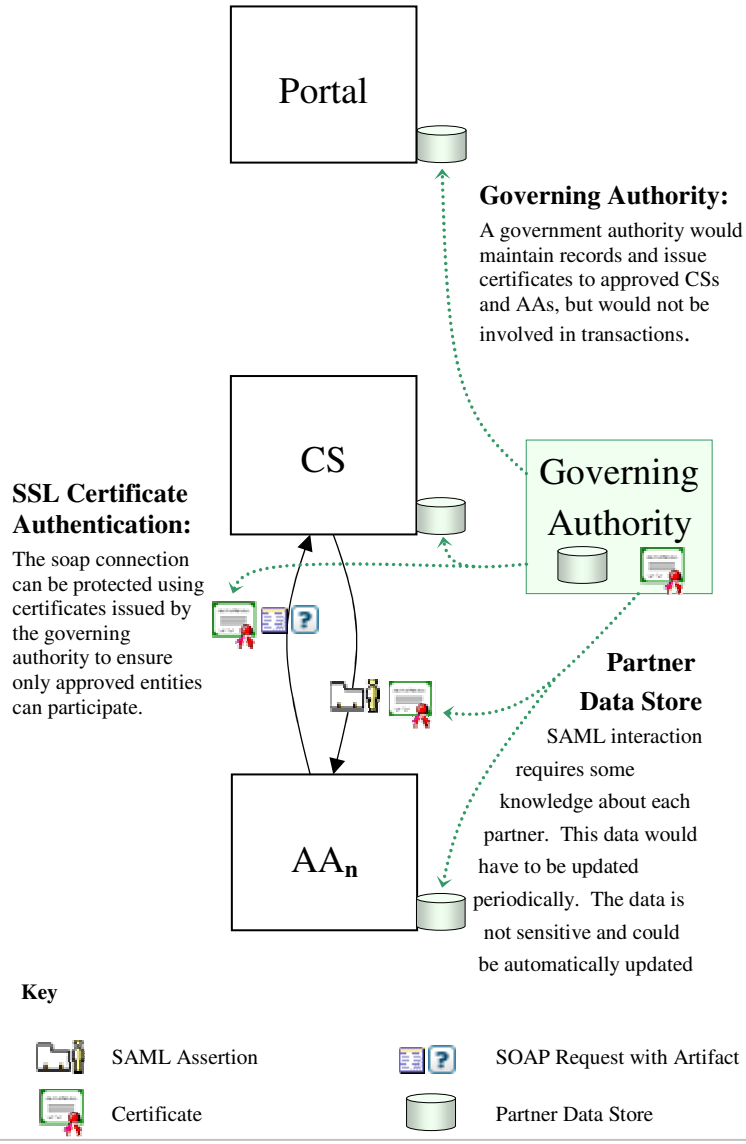
The redirects by the portal and CS should be extremely fast, and be nearly imperceptible to the user. From the users perspective they have simply typed in the URL of the AA and started to use it without needing to log in again.

4 GOVERNANCE

Any architecture for government-wide authentication would have to provide some mechanism for the government to assert its authority over which entities can participate. This section describes those mechanisms for this architecture.

The SAML specification allows for the retrieval of assertions over a client and server authenticated SSL channel. A governing authority established by the government could issue those certificates, effectively controlling which entities can participate. An CS attempting to make assertions without a certificate would not be trusted by AAs. Similarly, AAs attempting to retrieve assertions from CSs would not be trusted without the appropriate certificates. These certificates would be issued, renewed, or revoked periodically as determining by the authority.

Figure 3: Governance



SAML exchanges between two parties require each entity to have some knowledge about the other, such as partner IDs and SOAP URLs. The Governing Authority would have to maintain an authoritative copy of this information and make it available to the CSs and AAs. This information is not sensitive and not expected to change very often. The CSs and AAs would have to download the data periodically and update their configurations, ideally automatically. The SAML specification is silent on the distribution of this information, the government would have to determine and document this mechanism. It is unlikely the COTS products would support this functionality natively; custom modules would probably be required.

Neither of these governance functions involves the authority in each authentication transaction. They would focus on the policy and assessment tasks. AAs and CSs would interact directly with each other for daily authentication transactions using their government issued transactions.